The Vulnerability Analysis Project (VAP)

William J. Orvis

DOE Computer Security Conference

Seattle, April 22-26, 1996

UCRL-MI-123880

Work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

CIAC
Computer Incident Advisory Capability

What is VAP?

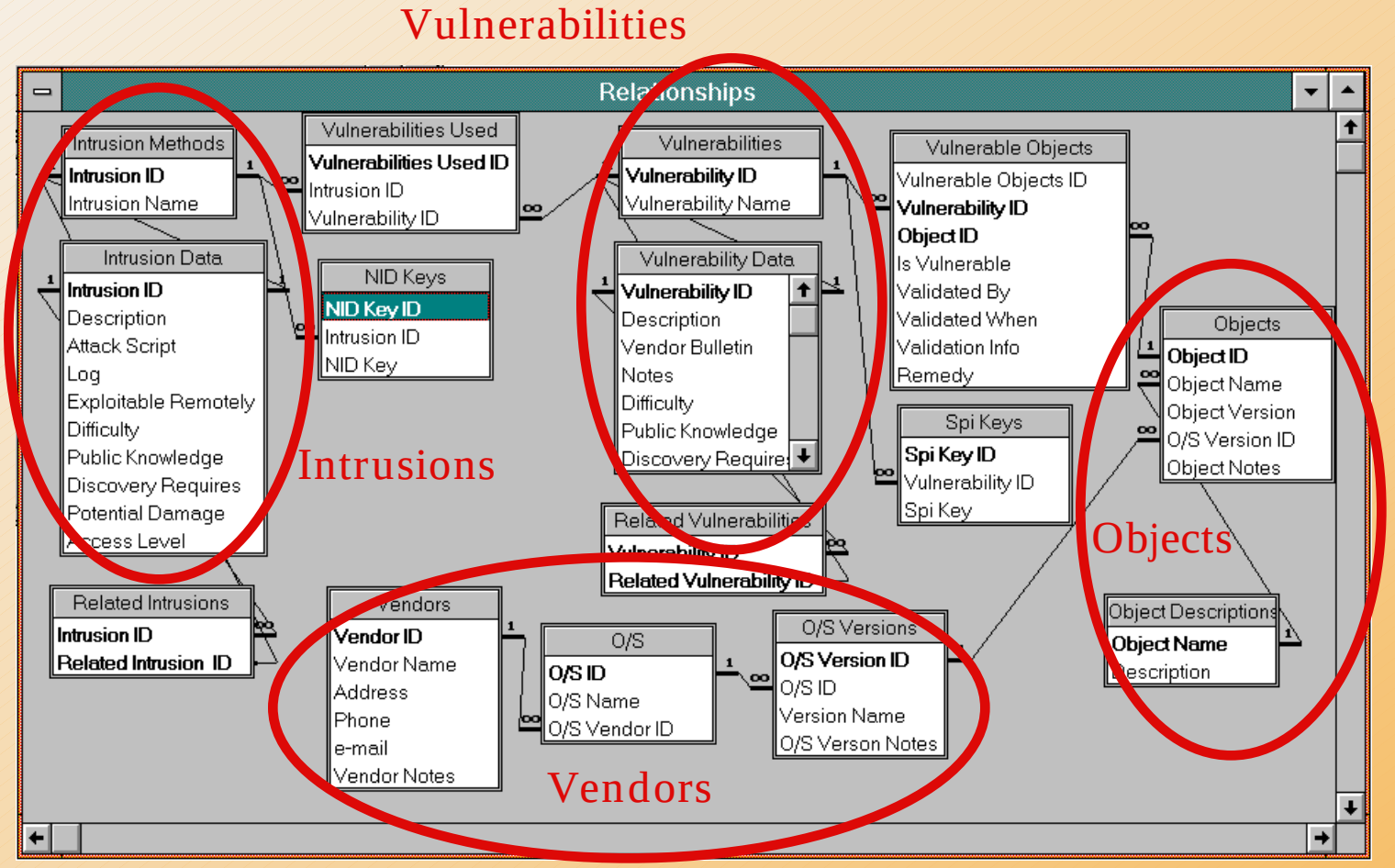
Vulnerabilities in modern computer systems and networks make it possible for unauthorized people to subvert security for malicious purposes. Systems today have many such vulnerabilities, with more being discovered daily.

- **VAP is a project to identify and catalog computer system vulnerabilities in a framework that can be used both for analysis of vulnerabilities and for incident response.**
- **VAP data structures are being coordinated with other response teams.**
- **VAP will be accessible to DOE security managers.**

The VAP Server Is In Place

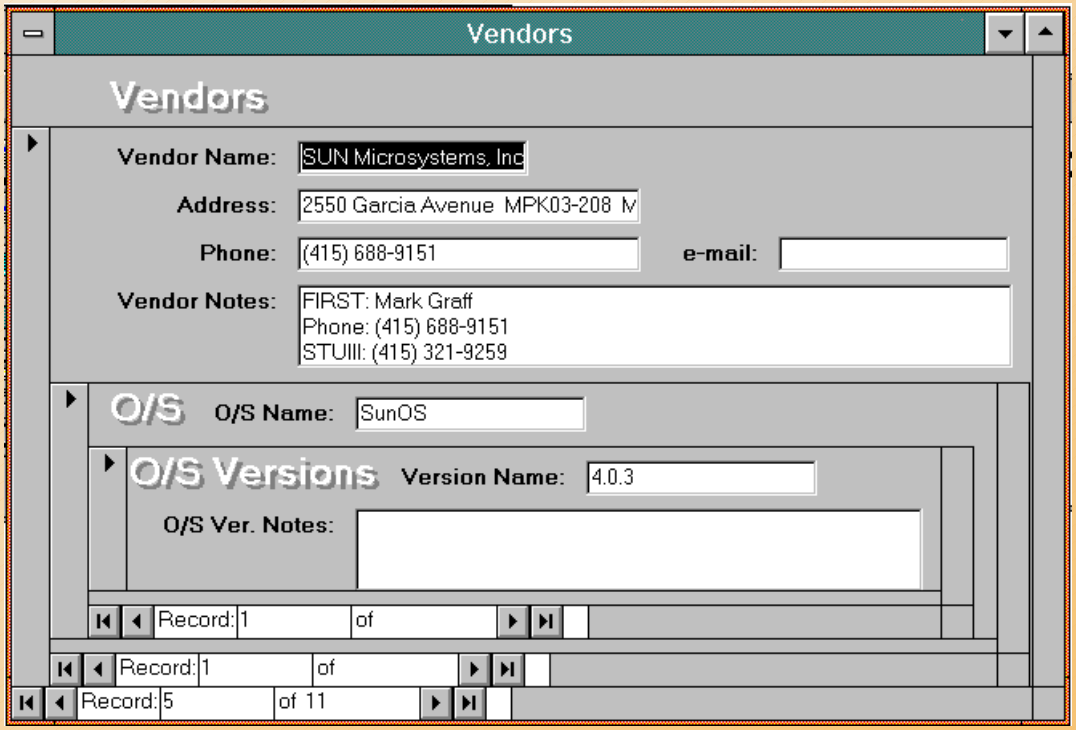
- **The server is based on a Sun Sparc 5 workstation behind the CSTC firewall.**
- **An Oracle server has been installed to hold the database.**
- **The database design is complete and implemented as an Access database.**
  - **Access was used to speed the initial development.**
- **The database is being populated.**

The Design Partitions the Information Into Four Distinct Parts



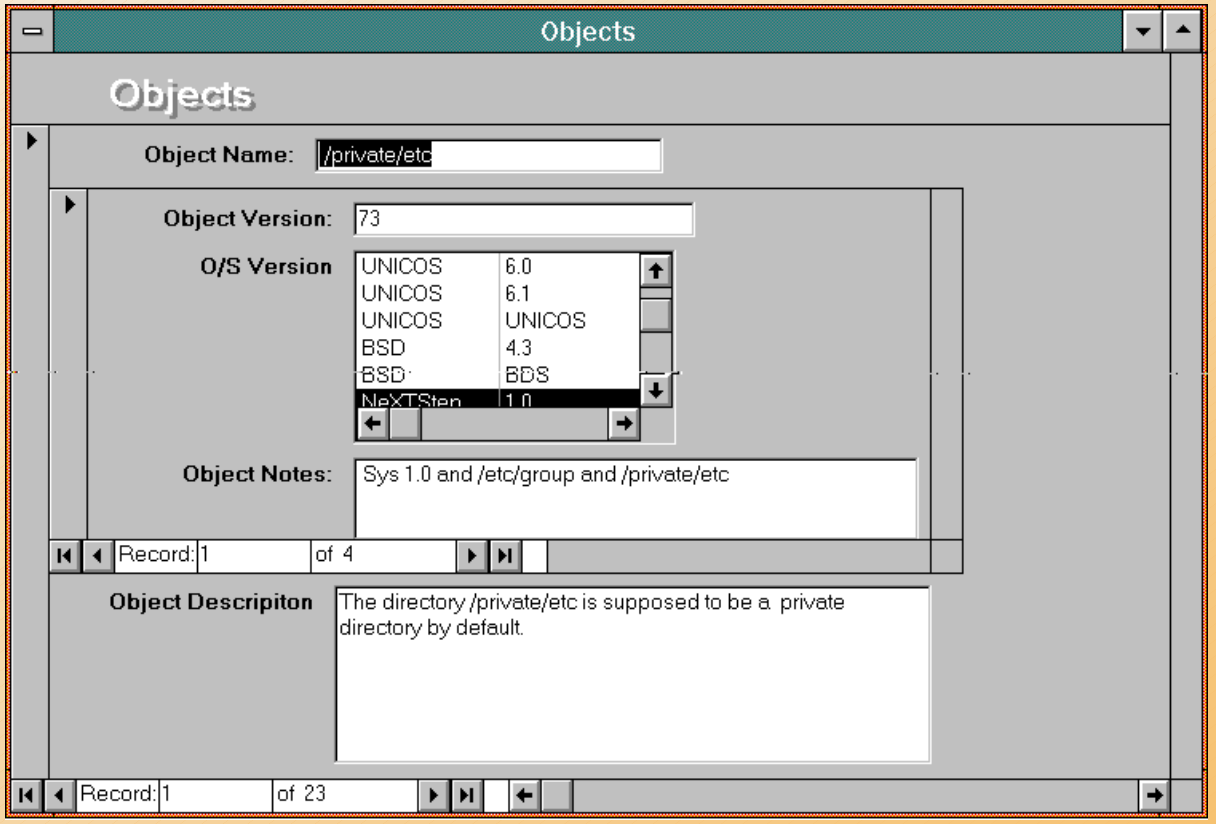
First: Vendor Information

- **The vendor information links the operating system versions and manufacturers.**



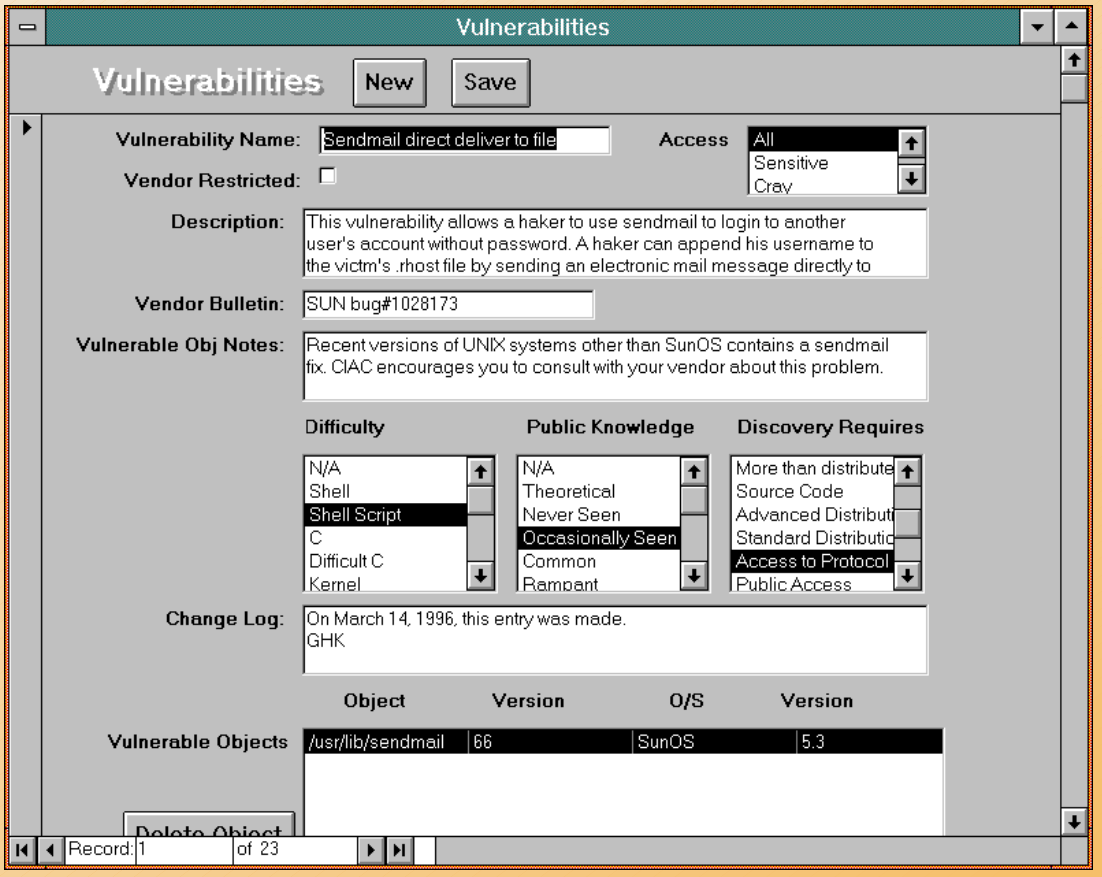
Second: Objects

- **The operating system objects are the files and structures that contain the flaw that allows the vulnerability to occur.**



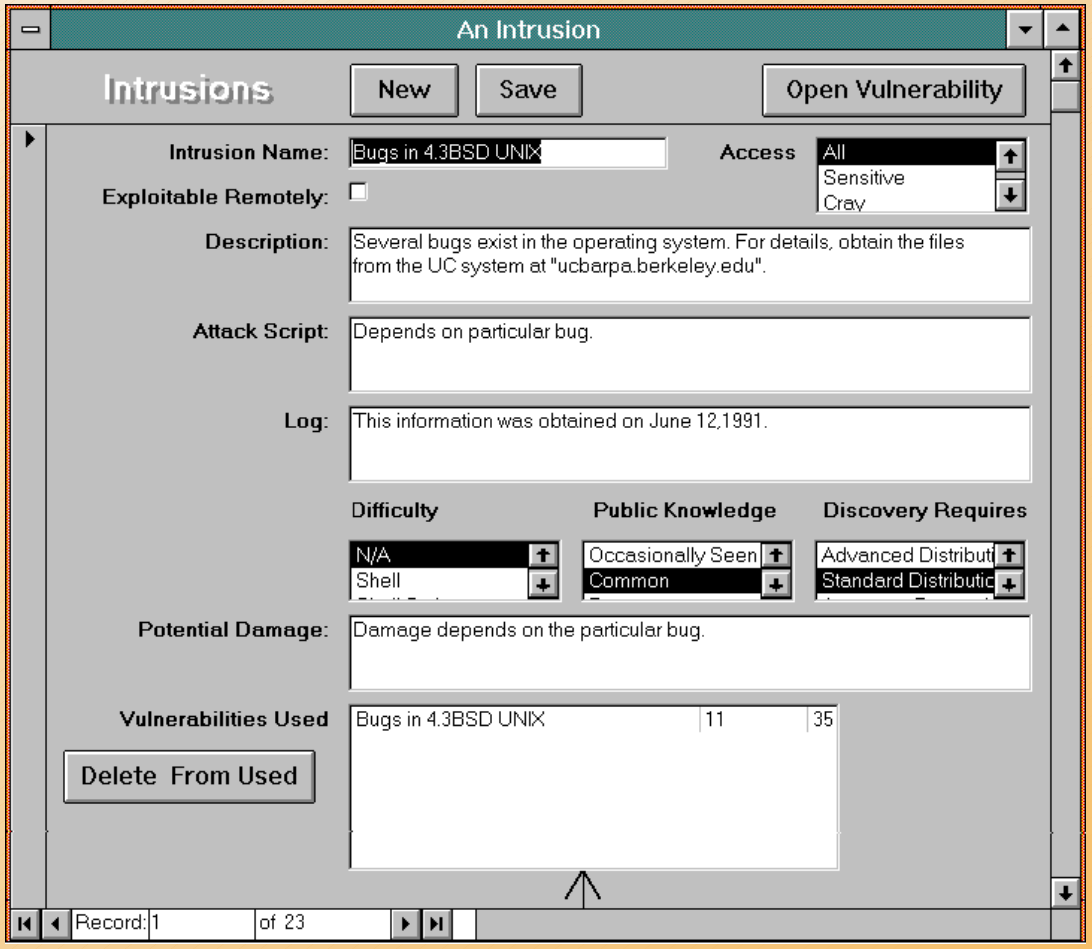
Third: Vulnerabilities

- **The vulnerabilities show how to exploit the flaw in the operating system object.**



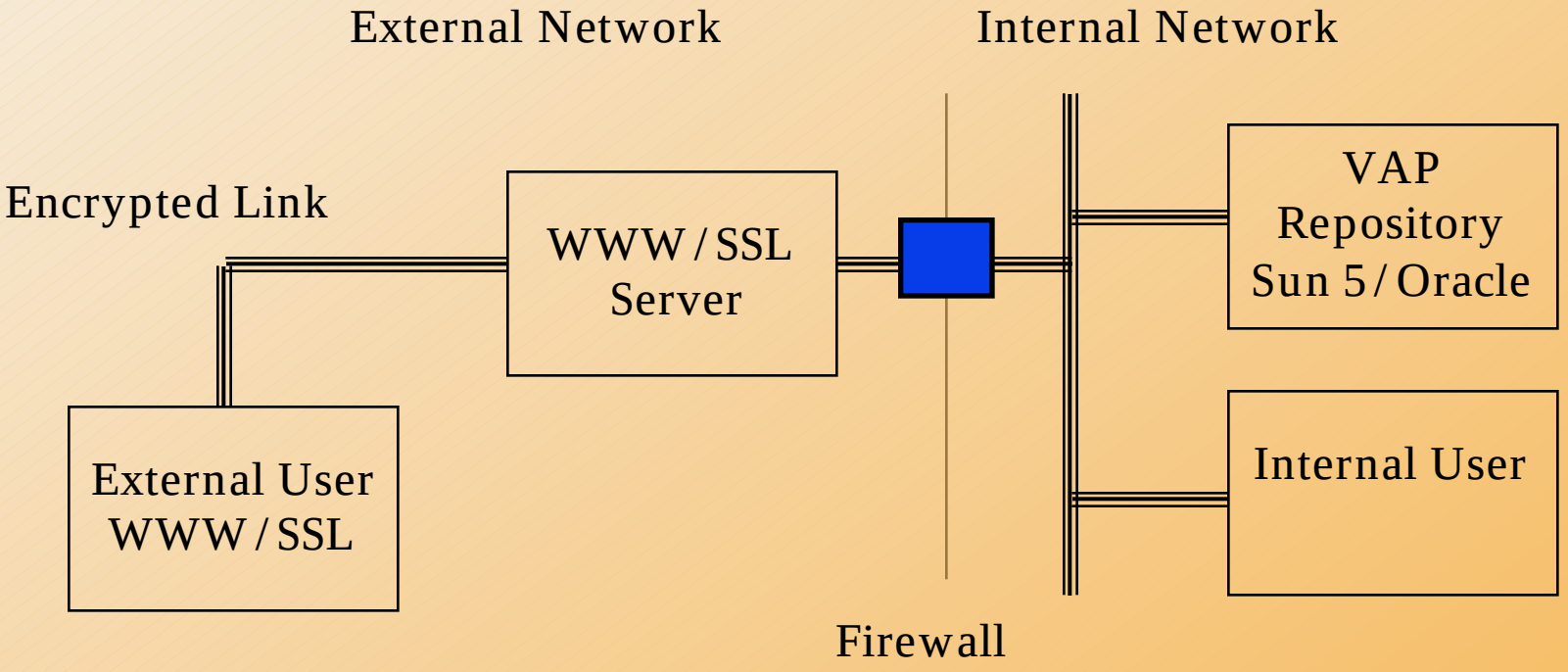
Fourth: Intrusions

- **The intrusions show how to exploit the vulnerabilities to gain unauthorized access.**



The Repository Is Protected

- **External users will use a web browser with an encrypted communication path.**
- **Access will be available to DOE security officers (*Real Soon Now*).**



VAP Is A New Security Resource

- **It will be available *real soon now* to DOE security managers.**
- **You will be able to search for vulnerabilities by name, system type, and other criteria.**
- **You will need world wide web access.**
- **You will need a browser that supports the secure socket layer (SSL) protocol.**
- **Access will be granted through your local DAA.**